

# **Additional Decoder Setup Instructions for IEC 60870-5-101, 102, & 104 Protocols**

---

Copyright © 2000-2009 Frontline Test Equipment, Inc. All rights reserved. You may not reproduce, transmit, or store on magnetic media any part of this publication in any way without prior written authorization of Frontline Test Equipment, Inc.

FTS, Frontline and Frontline Test System are registered trademarks of Frontline Test Equipment, Inc. Frontline is a trademark of Frontline Test Equipment, Inc.

All other trademarks and registered trademarks are property of their respective owners.

## Table of Contents

Setup Instructions for IEC 60870-5-101, IEC 60870-5-102 and IEC 870-5-104 Protocols _____	1
Decoder Parameters _____	1
IEC 60870-5-102 & IEC 60870-5-104 Application Layer Parameters _____	1
IEC 60870-5-102 Application Layer Parameters _____	1
IEC 60870-5-101 & IEC 60870-5-102 Link Layer Parameters _____	1
What To Do When The Correct Values Of Decoder Parameters Are Unknown _____	3
Link Layer Values _____	3
Application Layer Values _____	3

## SETUP INSTRUCTIONS FOR IEC 60870-5-101, IEC 60870-5-102 AND IEC 870-5-104 PROTOCOLS

NOTE: These instructions apply to IEC 60870-5-101, IEC 60870-5-102 and IEC 60870-5-104 only. IEC 60870-5-103 does not require any additional setup. For the remainder of the setup instructions, IEC 60870-5-101, IEC 60870-5-102 and IEC 60870-5-104 will be referred to as simply IEC 60870.

### Decoder Parameters

An interesting attribute of IEC 60870 is that the sizes of certain fields and the mode of transmission (balanced or unbalanced) must be specified by the user. Such values are called decoder parameters. Decoder parameters are set by the user in the Decoder Parameters dialog. To open this window, choose *Decoder Parameters* from the *Options* menu on the Control window.

The Decoder Parameters dialog displays automatically the first time that a capture file is loaded. The two tabs are titled “[protocol] Application Layer” and “[protocol] Link Layer” where “[protocol]” refers to the specific protocol.

### IEC 60870-5-102 & IEC 60870-5-104 Application Layer Parameters

“*Does Originator Address exist?*” specifies whether the application layer “*Originator Address*” field exists. Permissible values are Yes and No. The field is 1-byte long if it exists.

“*Size of the ASDU address field in bytes*” specifies the number of bytes in the application layer “*ASDU Address*” field. The permissible range is 1-2.

“*Size of info object address*” specifies the number of bytes in the application layer “*Information Object Address*” field. The permissible range is 1-3.

### IEC 60870-5-102 Application Layer Parameters

“*Size of the Integrated Total address field in bytes*” specifies the number of bytes in the application layer “*ASDU Address*” field. The permissible range is 1-2.

### IEC 60870-5-101 & IEC 60870-5-102 Link Layer Parameters

“*Is transmission balanced?*” specifies whether transmission is balanced or unbalanced. Permissible values are Yes and No. Balanced transmission mode is when two devices can both send at the same time. Unbalanced transmission mode is when only one device can send at a time. In the decode, three fields are affected by the transmission mode, and all are in the control byte of the link layer. Bit 8 is labeled “*Direction*” in balanced mode and “*Reserved*” in unbalanced mode. Bit 6 for secondary-to-primary is labeled “*Reserved*” in balanced mode and “*Access Demand for Class 1 Data Transmission*” in unbalanced mode. (For primary-to-secondary, the label is always “*Frame Count Bit*” regardless of transmission mode.) Bits 1-4 are always labeled “*Function Code*”, but have different values for balanced mode versus unbalanced mode.

*“Size of the address field in bytes”* specifies the number of bytes in the link layer *“Address”* field. The permissible range for the protocol itself is 0-2 in balanced mode and 1-2 in unbalanced mode, but the dialog will accept a range of 0-2 regardless of mode.

## WHAT TO DO WHEN THE CORRECT VALUES OF DECODER PARAMETERS ARE UNKNOWN

It is important to note that in many cases a useful decode can be obtained even if the correct decoder parameter values are unknown to the user.

### Link Layer Values

An incorrect value of the *“Size of the address field in bytes”* is easy to determine because fixed-length frames will be invalid and shown in red. The length of fixed-length frames is in the range 4-6. They begin with byte 0x10 and end with byte 0x16 (there can also be bytes with those values elsewhere in the frame). To correct the problem, change the values in *“Size of the address field in bytes”* field until fixed-length frames no longer appear in red.

An incorrect value of *“Is transmission balanced?”* has no effect on the rest of the decode, and it can be left as it is if the user doesn’t care about the three fields directly affected by it (see description above). There is no way to find the correct value by looking at the data, with the exception that if the size of the link layer address field is 0, then the transmission mode must be balanced.

### Application Layer Values

The application layer parameters are *“Does Originator Address Exist”*, *“Size Of ASDU Address Field In Bytes”*, and *“Size Of Info Obj Address Field In Bytes”*. They apply only to variable-length frames, which can be of almost any size. Variable-length frames start with byte 0x68, end with byte 0x16 (there can also be bytes with those values elsewhere in the frame), and come in two forms, identified by the value of the SQ bit, which is contained in the variable structure qualifier. The spec describes them this way:

SQ=0: There are one or more information objects, each with a single set of information elements.

SQ=1: There is only one information object, which contains one or more sets of information elements.

That's equivalent to saying this:

SQ=0: There is a separate information object address for each set of information elements.

SQ=1: There is one information object address and one or more sets of information elements.

When SQ=1, there is only one instance of the information object address, and finding a combination of values for the parameters that yields an otherwise valid decode is a generally simple matter of trial-and-error. If the detail pane indicates that there are extra data bytes (indicated by the presence of the Data field at the end), selectively increase the values of those parameters to use up the extraneous data. If the detail pane indicates that a field is missing, selectively decrease the values of those parameters until all fields are present. The fields that these parameters refer to are contiguous; therefore no intervening fields are compromised. What can make this process tricky is that some frames may in fact have the wrong number of bytes in them. When experimenting with parameter values, use frames which appear to be the same type and length as other frames in the decode since this generally indicates that those frames are of valid length.

When SQ=0, things are trickier. In this case, the information object address can appear multiple times, and not contiguously. It is technically possible to set the parameters such that there is neither extra Data nor missing fields but the decode itself is invalid. There is no surefire approach to this.